

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A computer system for establishing a certificate for use in the validation of a request sent between a pair of correspondents on a public key infrastructure, the system comprising:

an application located at one of said correspondents, said application generating a request;

a secure token in communication with said application, said secure token including a validation engine, a cryptographic engine, a certificate, and a private key; and

a certificate authority;

wherein said secure token receives said request from said application, authenticates the validity of said request through said certificate authority, said certificate is signed by said cryptographic engine using said private key, and said signed certificate is sent to a correspondent, where said certificate is known to be valid by said receiving node.

2. The computer system of claim 1, wherein said validation engine is invoked on each request to utilize said private key of said secure token.
3. The computer system of claim 1, wherein said certificate includes a certificate extension as a mechanism to indicate to said receiving node that said certificate is known to be valid.
4. The computer system of claim 1, wherein said secure token further includes a secure key, wherein said secure key is used to attest to the validity of said private key within said secure token and said private key is controlled by said validation engine each within said secure token.
5. The computer system of claim 1, wherein said validation engine enables the system to ensure said private key within said secure token is conformant with a specified policy.

6. The computer system of claim 1, wherein the validity of said certificate controls the use of said private key.
7. A method for establishing a certificate for use in the validation of a request sent between a pair of nodes on a public key infrastructure, the method comprising the steps of:
 - a) generating a request by an application located on said node;
 - b) sending said request to a secure token;
 - c) analyzing of said request by a validation engine located within said secure token;
 - d) sending said request to a certificate authority by said validation engine;
 - e) generating a certificate by said certificate authority ensuring the validity of said request;
 - f) receiving said certificate by said secure token;
 - g) executing said request by a cryptographic engine within said secure token using a private key located within said secure token, where said private key is associated with said certificate authority;

wherein the validity of said certificate is known to an intended receiving node.

8. The method of claim 7, wherein said certificate further includes a certificate extension signed by said certificate authority, and where said extension identifies to a receiving node the validity of said certificate.
9. The method of claim 7, wherein said token further includes a secure key such that on a request by an application said secure key attests to the validity of said private key located within said secure token.